

REMARKS/ARGUMENTS

Claims 1-48 are pending in the application. Claims 1-48 are rejected as anticipated under 35 U.S.C. 102(e).

Claim Amendments

Amended independent claims 1 and 25, respectively, propose a method and system of single sign-on user access to multiple web servers that involves authenticating a user and detecting a client request at a first web server. Amended claims 1 and 25 propose further that the first web server determines a second web server related to the request and in response thereto creates an encrypted, digitally signed authentication token with an expiration time related to the user, redirects the user's web browser to the second web server; and transmits the encrypted authentication token to the second web server via the user's web browser. In addition, amended claims 1 and 25 propose authenticating the authentication token at the second web server and allowing the user to conduct a session at the second web server. See, e.g., p. 2, line 12-p. 3, line 27.

Claims 1, 18, 39, and 42 are amended to address editorial issues raised by the amendment of independent claims 1 and 25; and claims 20-24 and 44-48 are canceled as a result of the amendment of claims 1 and 25. Support for the foregoing amendment is found throughout the specification and in the claims and as detailed above. Accordingly, no new matter has been added.

Claim Rejections - 35 U.S.C. § 102

Claims 1-48 stand rejected as anticipated by the Sasmazel (U.S. Patent No. 6,263,432) under 35 U.S.C. § 102(e). The rejection is respectfully traversed and reconsideration is requested. The reference asserted does not read on the claimed invention.

With regard to independent claims 1 and 25, the Examiner considers that Sasmazel discloses each and every claimed element. It is true that Sasmazel discloses authenticating a user by an authentication server when the user submits a sign-on request to a web server. According to Sasmazel, the web server sends the user's sign-on request to the authentication server, which validates the user's authentication information. See, e.g., Sasmazel, Col 8, lines 1-15 and Fig. 6. It is also true that Sasmazel discloses receiving a user's request, e.g., to initiate an "information discovery session". See, e.g., Sasmazel, Col 6, lines 10-39 and Fig. 2. In addition, it is true that when the web server of Sasmazel receives the user's request to initiate an "information discovery session", the web server gathers the information from data sources, such as a local database, a mainframe, or a "remote information discovery web server" coupled to the web server over a network. See, e.g., Sasmazel, Col 6, lines 10-39 and Fig. 2. It is likewise true that the authentication server generates and encrypts an "eticket" with expiration date and time. See, e.g., Sasmazel, Col 7, lines 38-67 and Fig. 5.

However, there is no teaching or suggestion whatsoever in Sasmazel of determining a second web server related to the user's request by a first web server and in response thereto creating an encrypted authentication token related to the user and redirecting the user's web browser to the second web server by the first web server, as recited in claims 1 and 25. On the contrary, instead of creating an encrypted authentication token related to the user in response to determining the second web server by the first web server, as recited in claims 1 and 25, according to Sasmazel, the eticket is generated and returned to the user's browser via the web server by the authentication server immediately when the user logs on to the web server. See, e.g., Sasmazel, Col 10, lines 9-30 and Fig. 7. Further, there is not a hint of teaching or suggestion in Sasmazel of likewise redirecting the user's web browser to a second web server in response to determining the second web server related to the user's request by the first web server, as also recited in claims 1 and 25.

Nor does Sasmazel teach transmitting the encrypted authentication token from the first web server to a second web server via the user's web browser and

authenticating the authentication token and allowing the user to conduct a session at the second web server, as recited in claims 1 and 25. On the contrary, while it is true that the eticket of Sasmazel is sent to the user's browser by the web server, instead of transmitting the encrypted authentication token to a second web server via the user's web browser, as recited in claims 1 and 25, according to Sasmazel, when the user requests an operation, the request and eticket are sent back to the same web server, which then sends the eticket to the authorization server for a determination of whether or not the user is authorized for the requested operation, and if so, simply executes the operation for the user. See, e.g., Sasmazel, Col 10, lines 9-30 and Fig. 7.

Rather than providing single sign-on user access to multiple web servers, according to claims 1 and 25, Sasmazel discloses an "eticket" system that allows a user to access a web server to initiate an "information discovery session" with an encrypted eticket including her authentication and authorization level, such that the web server can gather information from data sources, such as a local database, a mainframe, or a remote "information discovery" web server coupled to the web server over a network, without having to re-authenticate the user at each of the servers. See, e.g., Sasmazel, Abstract and Col 6, lines 10-39 and Fig. 2. Consequently, Sasmazel does not teach the required combinations of limitations of Applicants' method and system of single sign-on user access to multiple web servers, as recited in amended claims 1 and 25.

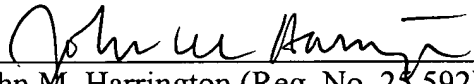
Because each and every element as set forth in amended claims 1 and 25 is not found, either expressly or inherently in the cited reference, the Examiner has failed to establish the required *prima facie* case of unpatentability. See Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628 (Fed. Cir. 1987); See also MPEP §2131. The Examiner has failed to establish the required *prima facie* case of unpatentability for independent claims 1 and 25 and similarly has failed to establish a *prima facie* case of unpatentability for claims 2-19 that depend on claim 1 and claims 26-43 that depend on claim 25, and which recite further specific elements that have no reasonable correspondence with the references.

Conclusion

In view of the foregoing amendment and these remarks, each of the claims remaining in the application is in condition for immediate allowance. Accordingly, the examiner is requested to reconsider and withdraw the rejection and to pass the application to issue. The examiner is respectfully invited to telephone the undersigned at (336) 607-7318 to discuss any questions relating to the application.

Respectfully submitted,

Date: 6/30/04


John M. Harrington (Reg. No. 23,592)
for George T. Marcou (Reg. No. 33,014)

Kilpatrick Stockton LLP
607 14th Street, NW, Suite 900
Washington, DC 20005
(202) 508-5800